the user may potentially require to interact with. Information supplied by the user is then used by the single sign-on services within the primary domain to support the authentication of the end user to each of the secondary domains with which the user actually requests to interact. The information supplied by the user may be, for example, stored in the cache and used at the time a request for a secondary domain services is made by an end user.

From a management perspective, a single user account management interface is provided through which all component domains may be managed in a coordinated and synchronized manner. For the integration to work, the secondary domains have to trust the primary domain to correctly assert the identity and security attributes of the end user and protect the authentication information used to verify the end user identity. In addition, the authentication information is protected when transferred between the primary and secondary domains. However, Applicant is unable to find the alleged teaching in the office action regarding providing a configurable security key manifest operative to contain a non-specified number of security keys. For example, page 3 does not appear to be directed to a security key manifest of any type. Moreover, the office action cites pages 110 and 114 for allegedly teaching, for example, in page 10 for allegedly teaching accepting new key attribute data to produce a configured security key manifest and dynamically controlling through a configured security key manifest, a generation of at least one new security key for the subscriber based on received key attribute data contained in the configured security key manifest. However, upon review of page 10 for example, it merely teaches that a cache is used as temporary store sign-on information associated with a given user. There is no teaching or suggestion, for example, of the claimed steps.

In addition, pages 14-17 and 38 have been cited as allegedly teaching authentication procedures that apparently require, the using a configured security key manifest to dynamically

control the generation of a new security key for a subscriber based on a received key attribute data contained in the configured security key manifest. However, the cited portions of the reference do not appear to teach a configured security key manifest that is produced based on the new key attribute data or using a configured security key manifest to dynamically control the generation of a new security key for the subscriber based on received key attribute data. The cited pages again to do not appear to describe how new keys are generated, but instead indicate that an authentication token associated with the user can be changed. The mechanism for how this is done does not appear to be described. Therefore, Applicant respectfully submits that the independent claims are in condition for allowance. However, if the rejections are maintained, Applicant respectfully requests a showing as to which language appears to anticipate the specific claim language alleged to be taught in the reference.

Applicant also respectfully submits that the dependent claims add additional novel and non-obvious subject matter.

Accordingly, Applicant respectfully submits that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: August 12, 2004

By: 
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P. C.
222 N. LaSalle Street
Chicago, IL 60601
PHONE: (312) 609-7500
FAX: (312) 609-5005